doi :10.3969/j.issn.1671-1122.2018.08.004

一种基于区块链的分布式公钥管理方案研究

刘敬浩[1]，平鉴川[1]，付晓梅[2]

（1. 天津大学电气自动化与信息工程学院，天津 300072；2. 天津大学海洋科学与技术学院，天津 300072）

摘　要：分布式系统相对于集中式系统，存在系统中难以达成一致共识的难题，因此分布式系统在信息存储相关应用上受到很大的限制。区块链的出现和对其研究的深入为在分布式系统中建立共识给出了一个较为可靠的实现方式。文章提出建立一个基于区块链技术的分布式公钥方案，通过区块链网络中的节点共同承担密钥存储的职责。通过将存储系统拆分到网络的组成节点中，相较于传统的中心化公钥系统能够提供较好的响应性能和抗干扰能力。对于区块链系统在虚拟货币中应用时已经显现出的缺陷，在分析了这些缺陷对公钥管理的影响后，通过对区块链系统进行一定的改进进行规避。最后，文章对一些常见的针对公钥系统的攻击方式进行了分析，证明了系统对攻击者通过欺骗节点干扰共识的达成和传播有着较强的抗干扰性，保证了公钥管理系统的安全性。

关键词：区块链；密钥管理；分布式系统；公钥密码

中图分类号：TP309　**文献标识码：**A　**文章编号：**1671-1122（2018）08-0025-09

中文引用格式：刘敬浩，平鉴川，付晓梅. 一种基于区块链的分布式公钥管理方案研究[J]. 信息网络安全，2018，18（8）：25-33.

英文引用格式：LIU Jinghao, PING Jianchuan, FU Xiaomei. Research on A Distributed Public Key System Based on Blockchain[J]. Netinfo Security, 2018, 18 (8): 25-33.

Research on A Distributed Public Key System Based on Blockchain

LIU Jinghao[1], PING Jianchuan[1], FU Xiaomei[2]

(1. *School of Electrical Automation and Information Engineering*, *Tianjin University*, *Tianjin* 300072, *China*; 2. *School of Marine Science and Technology*, *Tianjin University*, *Tianjin* 300072, *China*)

Abstract: Compared with centralized system, distributed system has difficult in reaching consensus in the system. Therefore, distributed systems are greatly limited in application of information storage. With the advent of the blockchain and its further research, a more reliable implementation is given for establishing consensus in distributed systems. In this paper, we propose a distributed public key scheme based on blockchain technology, which shares the key storage responsibility through the nodes in the blockchain network. By splitting storage system into constituent nodes in the network, it can provide better response performance and anti-interference capability than

收稿日期：2018-1-15

基金项目：国家自然科学基金 [61571323]

作者简介：刘敬浩（1963—），男，天津，副教授，硕士，主要研究方向为网络安全、网络虚拟环境、无线网络通信；平鉴川（1994—），男，浙江，硕士研究生，主要研究方向为网络安全；付晓梅（1968—），女，重庆，副教授，博士，主要研究方向为无线通信、海洋通信、信息安全。

通信作者：平鉴川 764463703@qq.com

the traditional centralized public key system. For the shortcomings that have appeared in the application of the blockchain system in the field of virtual currency, after analyzing the impact of these defects on the management of the public key, some blockchain system is avoided by some improvements. At the end of the article, some common attacks on public-key systems are analyzed. The results show that the system has a strong anti-jamming effect on the aggressors' System security.

Key words: blockchain; key management; distributed system; public key

0 引言

非对称加密算法由 DIFFIE[1] 等人于 1976 年提出，也被称为公开密钥密码体系。这种加密算法突破了对称加密算法的局限，解决了利用对称加密算法难以解决的两个难题：密钥管理难度大以及难以实现信息的不可否认性（non-repudiation）。由于非对称密钥算法的复杂度普遍高于对称密钥算法，加密速度远远低于对称加密算法，因此目前实际应用中多采用综合两种算法的混合密码体系，即使用公钥密码保护随机生成的通信密钥，用对称加密的方式加密信息。

在公钥密码体系中，一个难题在于如何保证用户获得的公钥和通信目标节点的公钥保持一致，也就是公钥认证问题。为了避免公钥信息被攻击者篡改，建立合适的公钥系统能够降低节点的公钥信息被篡改的风险。目前主流的公钥认证的解决方案有公钥基础设施（Public Key Infrastructure, PKI），基于身份的密码系统（Identity-based Cryptography）以及无证书公钥密码系统（Certificateless Public Key Cryptography）3 种。在实际使用的过程之中，每种解决方案也会存在一定的操作风险。

公钥基础设施是一种传统的公钥密码解决方案，系统中包含了认证机构、仓库和多个用户节点。认证机构也被称为中心节点（Certificate Authority, CA）。认证机构的职责是为用户签发公钥证书，用户基于对认证机构的信任相信认证机构颁发的证书。仓库负责存储认证机构签发的证书。当系统较大时，认证机构会采用层级结构构建，即上层认证机构签发下层认证机构的公钥证书，基于对上层认证机构的信任，用户信任下层认证机构签发的证书。这种方案能够较好地解决公钥认证的问题，只是当一个认证机构被入侵后，可能存在认证机构滥发证书、认证机构被注销造成正常证书失效、存在不可信的认证机构的情况，会使得正常用户对整个系统产生信任危机。

基于身份的密码体系 [2] 是一种将用户信息作为公钥，以实现用户和公钥信息绑定的方案。在基于身份的密码体系中，系统由私钥生成中心（Private Key Generate Center, PKG）和用户节点组成。生成密钥时，用户向私钥生成中心提供自身的身份信息（ID），私钥生成中心在收到用户的身份信息后利用主密钥生成用户的私钥，并将私钥发送给用户。其余节点可以使用用户的身份信息作为公钥加密信息，用户可以通过得到的私钥来解密信息。这种方案使用用户的身份信息作为公钥，从本质上解决了公钥认证的难题。但是由于方案的特点，引入了一些新的安全问题。

1）在私钥传输的过程中，攻击者可以通过窃听获得用户的私钥；2）由于所有用户的私钥都由私钥生成中心生成，私钥生成中心掌握所有用户的私钥信息，这也被称为私钥托管问题，一旦攻击者成功入侵私钥生成中心，攻击者能够利用私钥生成中心的资源破解所有节点的密钥；3）为了便于系统正常运行时节点之间的识别，往往采用用户不会变化的公共信息作为公钥或公钥的组成部分。当用户私钥泄露或被攻击者以某种方式获得，用户在新的密钥的选择上将会受到很大的限制。

无证书公钥密码系统 [3] 是为了克服基于身份的密码体系引入的新问题而提出的解决方案。和基于身份的密码体系类似，无公钥证书系统也存在一个中心节点，称为密钥生成中心（Key Generation Center, KGC）。

与基于身份的密码体系区别在于在密钥生成过程中，密钥生成中心利用主密钥和节点的信息生成部分私钥发送给用户，用户利用接收到的部分密钥在本地生成自己的密钥对。这种算法克服了基于身份的密码体系中私钥传输和私钥托管的问题，密钥生成中心不掌握用户的私钥信息。由于用户的公钥由用户生成，需要通过其他方法来解决公钥认证的问题。由于密钥对的生成方式复杂、需要较多的信息，要求密钥生成算法存在多个可分离的运算步骤。较为复杂的加密算法存在设计缺陷的概率也较高，使得加密效果无法达到预定目标。

相对于分布式系统抗干扰性高、响应速度快的优势，分布式系统存在难以在网络中达成共识的问题。目前主要的公钥认证的解决方案都采用中心化的系统布局，对中心节点的安全性、运算能力等都有着较高的要求。本文提出的在区块链上建立的公钥认证系统，通过将系统中的运算和存储能力分散到网络中的众多节点中去，实现在各个节点达成共识，利用分布式系统的优势提供对查询请求的快速响应。由于节点中存有的信息多数为公开信息，因此部分节点被恶意节点攻击不影响系统的正常运作。

区块链技术也被称为分布式账簿技术（Distributed Ledger Technology），用于在分布式的网络中构建起节点之间的共识。相对于中心化系统，分布式系统存在共识难以达成的问题，也被称为拜占庭将军问题[5]。攻击者可以通过欺骗分布式系统中的部分节点，使得分布式系统中存储的信息无法达成一致。区块链技术在一定程度上解决了拜占庭将军问题，如果攻击者只是简单地发布虚假的信息，受骗的节点在收到新的信息时会发现异常，尝试将存储的信息和整个系统保持一致。当系统对某个信息达成共识之后，攻击者无法轻易篡改该信息的内容。通过在区块链上建立一个合适的公钥系统，能够利用区块链的不可更改的特性来解决公钥密码体系中的公钥认证问题。

1 预备知识

1.1 区块链技术

区块链技术由化名为“中本聪”的人在 2008 年提出比特币[4]的概念时同时提出，用于保障比特币账本的安全。由于比特币体系中不存在货币标志物，通过比特币账本记录交易中比特币的流向，以此通过计算了解用户拥有的比特币的数量，因此比特币的安全性高度依赖比特币账本的安全状态。在比特币系统中，比特币账本通过区块链来记录，区块链的结构如图 1 所示。区块链延伸一个区块，就代表有一定量的比特币交易被区块链所记录。

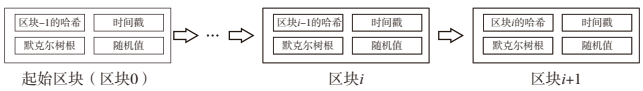

图 1 区块链结构

区块链作为一种分布式的系统，在运行时相对于各个节点存储的信息需要有一个协商的过程。分布式系统信息的不可更改性建立在协商建立的共识不可更改之上，攻击者通过攻击少数几个节点无法更改系统中建立的共识。协商过程会造成信息存储的速度要慢于中心化的系统，同时需要保证正常节点的协商结果不会因为恶意节点的干扰而产生不一致结果。

区块链具有信息加密、网络开放以及不可更改的特点[6]。受虚拟货币的影响，目前关于区块链的应用集中于金融领域，关于区块链在其他方向上的应用也受到研究者的关注[7]。在早期区块链技术的研究往往依赖于虚拟货币，随着研究的深入，关于区块链的研究已经逐渐从虚拟货币的方向分离开来成为一个独立的研究方向[8-13]。许多基于区块链的应用也开始出现[14-18]，尝试在虚拟货币之外的情景中对区块链技术加以应用[19-21]。

区块信息由所有节点共同参与维护，每个节点具有对等的地位，通过区块链的延长来存储信息以及保护区块的不可篡改性，每个区块由区块头和区块体组成。区块头中包含前一个区块的哈希值、区块体的默克尔树（Merkle Tree）根、噪声值和一些区块相关的

信息。

区块体为默克尔树，其中存储着一段时间内从区块链网络中接收到的信息。区块链中的节点通过完成区块证明来生成区块，或称为发现区块。为了避免攻击者通过生成伪造的区块来攻击区块链系统，区块链对一个区块的生成有一定的难度要求，目前运行的区块链系统中主要有工作量证明（Proof of Work, PoW）、股权证明（Proof of Stake, PoS）[8] 以及委任权益证明（Delegated Proof of Stake, DPoS）[9]3 种证明方式。工作量证明方式是系统设定一个难度目标，当计算出的区块头的哈希值小于目标难度，就认为这个区块是一个合法区块；股权证明方式是为了解决工作量证明方式计算消耗大而提出的，证明方式是记录用户持有的价值物的时间，当用户持有价值物时间越久，发现新的区块的难度就越低，而且当节点发现一个新的区块后，持有价值物的时间清零，重新开始累积；委任权益证明区块生成方式类似于股权证明方式，区别在于委任权益方式中有权力生成区块的节点为少数由所有节点选举出的节点。

这 3 种方法避免了攻击者能够通过较小的代价更改区块链中存储的内容。而且当系统具有较大规模时，参与维护的节点越多，篡改一个区块付出的代价也就越大。

1.2 区块分叉

区块头中包含的哈希值确定自身的前驱区块，每个区块只有一个前驱区块。在区块链中，从根区块开始长度最长的区块称为主链。考虑到网络传输存在延时，当多个节点同时独立生成区块时，生成的多个区块拥有共同的前驱区块，这在区块链中称为分叉。在正常情况下，当主链上产生分叉时，传播范围较广，拥有较多运算力的分支会比其他分支更快生成新的区块，从而更快地延长主链。在其他链上工作的区块接收到新生成的区块后，由于最长链发生变更，会迁移到新的主链上进行工作，主链的运算力优势进一步扩大，直到所有节点都在主链上进行工作。由于分叉问题的存在，从节点的角度观察，一个区块在加入主链后可能会被其他区块所替代，这个概率随着主链的延长，后继区块数量的增加而降低。因此一个信息并不能在被区块链记录后的第一时间就被确认，通常需要延后一段时间才能认为信息不会被更改，延后的时间根据信息的重要程度由与信息相关的人协商权衡所确定。由于这种信息延后确认的机制存在，攻击者在篡改信息前需要等候包含篡改目标信息的区块之后产生若干个区块，使得受害者误认为信息已生效。由于生成一个区块链需要耗费一定的资源，持续比系统更快地生成多个区块对攻击者是一个重大的挑战。

1.3 默克尔树

在区块中，信息以默克尔树的形式存储在区块体中，由默克尔树保证信息的安全。默克尔树也是一种哈希树（Hash Tree），它是一类特殊的二叉树，结构如图 2 所示。每一层节点为子节点数目的一半（向上取整），除每一层最后一个节点，所有节点都有两个子节点。叶节点存储信息的哈希值，非叶节点为其子节点值组合的哈希值，当节点只有一个子节点时，节点的值为子节点自身重复组合的哈希值。从叶节点到根节点的路径上非叶节点的另一个子节点的组合称为一个默克尔分支。区块头中包含默克尔树根，节点在获得信息后，通过默克尔分支可以快速地验证信息是否正确。

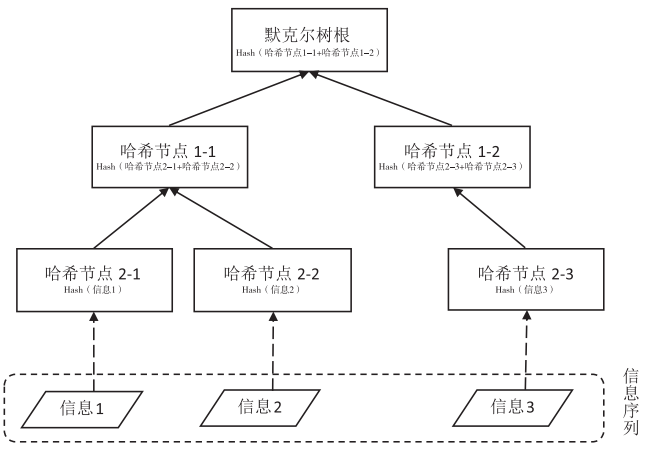

图 2 默克尔树示意图

1.4 哈希函数

哈希函数的作用是将任意长度的信息转换为固定长度的散列信息，一个可靠的哈希算法需要具有单向性（one-way）、弱抗碰撞性和强抗碰撞性（统称为抗碰撞性，Collision Resistance）。其中单向性指通过散列值反向计算出消息是无法实现的。弱抗碰撞性指当拥有一条消息时，找到和拥有的消息具有相同哈希值的另一条消息是难以实现的。强抗碰撞性指的是找到拥有相同哈希值的两条消息是难以实现的。

2 方案介绍

本文方案通过在区块链上建立一个公钥分发系统，利用区块链上的共识建立体系，来保障公钥分发过程中网络中的所有节点能存储记录一致。当信息被区块链记录后，区块链的抗更改特性能够保障公钥和节点之间的对应关系。当用户向区块链网络请求公钥时，能够通过区块链网络来验证获得的公钥信息是否真实。

系统由多个核心节点参与区块链的维护，各个节点之间处于对等关系。核心节点下包含若干个用户节点，用户节点不参与系统的运作，享受核心节点提供的公钥服务。用户生成自己的通信密钥后，通过核心节点托管到区块链系统中。核心节点的职责包括生成新的区块、存储部分密钥以及对密钥请求做出响应。在系统中核心节点不像公钥基础设施的仓库一样需要存储所有的公钥信息，只需要存储系统中部分用户的公钥信息。为了保证用户的公钥在收到查询请求时，必定会有节点做出响应，节点存储区块需满足以下的逻辑：当区块中包含委托节点管理的用户的公钥时，节点保留完整的区块；否则，节点只保留区块头，丢弃区块体。

2.1 密钥生成

用户加入区块链时，在本地生成用户自身的公钥和私钥。公钥信息包含用户 ID、用户公钥、时间戳、公钥的有效起止时间。公钥信息经核心节点密钥签名后，通过核心节点发布到区块链网络中。其余核心节点通过网络接收到公钥信息后，将信息加入缓存队列中。当节点开始生成区块时，从缓存队列中提取若干公钥信息，在验证公钥信息有效性后添加到新的默克尔树中，作为区块体。当核心节点发现一个合法的区块之后，向所有节点广播发现的区块。其余节点在收到广播的区块之后验证区块是否合法。在通过合法性检查之后，将区块加入区块链中，并根据区块中包含的信息，调节信息的缓存队列并从调节完成后的缓存队列中选择下一个区块中包含的信息。节点是否保留区块体取决于其中是否包含需要保存的公钥。

为了避免用户在托管时限之后继续占用区块链服务，节点生成一条用户托管时限的信息。该信息包含用户 ID、用户托管时限的起止时间，该信息经过节点签名之后发布在网络中，通过区块链存储。

由于区块链系统信息确认存在延后性，因此当包含用户的公钥的区块刚被包含进区块链的主链中时，有一定的概率会被支链中的区块所替换，因此此时区块中的信息处于不可信的状态。随着新的区块不断加入区块链，主链不断延长，区块被支链所替换的风险不断降低，当这概率低于用户预期的风险时，可以认为此时区块链中的信息是可信的。

2.2 公钥查询

当用户向节点请求公钥信息时，节点先在本地寻找是否存在用户请求的公钥。节点从区块链主链的末端开始向前查询，遇到有效的信息就结束查询。如果本地存在相应用户的信息，直接将公钥信息返回给用户。

当本地不存在对应用户的信息时，节点在区块链网络中请求公钥信息。收到请求的区块链节点检查本地存储的公钥信息。若存储有相应公钥信息，节点会返回对应的公钥信息以及包含公钥信息的区块和默克尔树分支信息。发起请求的节点在收到公钥信息后，通过多个节点返回的公钥信息和默克尔树分支之间交叉验证来确认公钥信息正确性。在确认获得的公钥

的可靠性后，节点将公钥信息发送给用户。

2.3 密钥更新

密钥更新的流程和密钥生成相似，由于用户在区块链中已有可用的公钥，更新密钥不需要经过核心节点的签名。当用户需要更新密钥时，在本地生成新的密钥对，使用旧的密钥对新的公钥信息进行签名，并发布在区块链网络中。由于节点在查询密钥时只选择最新的有效密钥，用户的旧密钥在新密钥生效后自动失效，成为无效公钥。当一个区块中所有信息都为无效信息且不存在前驱区块时，这个区块不再具有价值，节点不需要再维护这一区块。由于区块链确认信息的延后性，因此在替换密钥时，用户需要提前将新的密钥提交到区块链网络中。在系统正常运行的情况下，用户在旧有密钥失效前提交新的密钥，当新密钥开始进入有效运作时间前，新密钥已经得到广泛的认可。

2.4 密钥注销

在系统运行时，考虑到存在用户密钥因被恶意攻击者窃取、用户不再需要公钥服务等原因，需要注销存储在区块链系统中的公钥的场景。在这种情况下，用户可以选择等待密钥自动过期，也可以选择主动注销密钥。密钥注销过程由用户生成一个包含空密钥的信息，使用最后有效的公钥进行签名。当其他节点在区块链中检索到这条信息时，表明该用户已经注销自己的公钥。

3 方案分析

在虚拟货币的实际运行中，也发现了区块链系统存在的一些缺陷。主要有资源消耗高、信息存储速率受限以及信息确认存在延时这 3 类问题 [19]。

1）由于信息在被存储入区块链后并不能在第一时间得到确认，因此信息处理的速率会受到限制。在虚拟货币系统中，这个问题对虚拟货币的推广应用会有较大的影响，因为区块链中生成一个区块平均需要 10 分钟的时间，确认一笔交易大约需要 1 小时左右的延时，并且区块链处理交易的速度不足每秒 10 条。因此区块链体系处理交易的速度远远无法和传统的中心化的金融服务相比较。如果将区块链技术应用于密钥保护，这个问题对系统运行的影响远小于在金融领域的应用，而且通过合理设计系统可以避免负面影响。由于公钥的有效期一般较长，因此在公钥认证方面有一定的延时对节点的运作影响较小。当有较多节点参与区块链的维护时，区块链生成新的区块的时间趋于稳定，区块确认的时间也趋于稳定，当区块需要更新密钥时，在时间上有合适的提前量能保证密钥能够稳定地更新。

2）在虚拟货币系统中，确认用户拥有的虚拟货币数量需要追溯用户所有的账本，因此随着时间的积累，存储区块链信息所需的空间也变得巨大。目前比特币的全节点需要存储大约 130 GB 的数据，不同的虚拟货币之间因为出现时间、交易频度的不同存在一定差异，也存在存储空间膨胀的问题 [10]。而在公钥系统中，和金融系统最大的区别在于节点的运行不需要历史信息。在虚拟货币的系统中，每一笔交易都是有效信息，因为这些交易影响到用户拥有虚拟货币的数额。而在公钥系统中，每一个用户应当只对应唯一的一个公钥，因此节点的历史公钥信息并不具有价值。当一个区块中包含的信息随着时间流逝失去价值时，这个区块也没有继续被存储的必要了。节点在寻找主链的过程中可以通过删除无价值的区块来避免因时间流逝区块链的大小扩大引发的存储危机。而且删除无价值的区块还会使得区块链能够更为灵活的升级算法。随着计算性能的不断提升以及对哈希算法破解的不断研究，为哈希算法创造碰撞所需的花费在不断下降，当现有的哈希算法存在潜在威胁时，可以较为平稳地过度到新的哈希算法。当旧有区块在失去价值从区块链中剔除后，不会因旧有的区块存在算法漏洞而威胁到后续的区块的安全。

3）为了维护区块链系统，避免信息被篡改，需要节点不断收集信息，生成新的区块。采用工作量证明方式的区块链，在这个阶段会消耗大量的运算能力；

采用股权证明方式的区块链中，由于节点生成新的区块较工作量证明方式较容易，节点资源耗费较少，因此节点会有较高的倾向在多个链上同时工作，当区块产生分叉时，节点会更倾向于在两个分叉上同时工作，干扰信息的唯一性。综合两种区块证明方式，由于系统的目标是解决公钥认证问题，对保证信息唯一性的目标高于减少系统对资源的消耗，因此在本文设计的系统中采用工作量证明的方式作为区块合法性的检验标准。

4 安全性分析

本文系统通过利用区块链的安全性来保障运行于区块链上的公钥分配系统的安全。关于区块链的安全性分析已经经过前人的证明，研究者对于区块链系统潜在的威胁进行过比较深入的分析。攻击者需要付出极高的代价来篡改区块链中的信息。以下是对几种潜在的威胁的分析。

4.1 哈希碰撞

区块链系统的安全性主要由哈希函数的安全性作为保障，主要利用哈希函数的弱抗碰撞性来避免攻击者寻找一个和攻击目标具有相同哈希值的数据来篡改信息。在区块链中，使用哈希函数保护系统主要在 3 个方面：验证区块是否合法、寻找前驱区块、验证默克尔分支合法性。其中而验证区块是否合法只要求计算得到的哈希值小于目标值即可。后两个应用要求目标哈希和通过计算得到的哈希保持一致，即需要攻击者构建一个哈希碰撞。目前攻击者已经能够对较弱的哈希函数（如 MD5[11] 和 SHA–1[12]）构建碰撞攻击。目前使用改进后的 Shattered 算法构建一个 SHA–1 的哈希碰撞仍然需要进行 2^{63} 次 SHA–1 运算，需要耗费单一 GPU 一年的运算量 [13]。对 SHA–1 的理论攻击算法最早由 WANG[14] 等人在 2005 年提出，随着研究的深入和计算机性能的提升，在 12 年后实现了 SHA–1 的碰撞。作为对比，MD5 算法从缺陷发布到碰撞实现经历了 9 年的时间。目前对于 SHA–2 等较强的哈希函数并没有提出可行的碰撞算法，可以认为只能通过暴力猜测进行破解，因此在现有条件下可以认为构建一个较强哈希函数的哈希碰撞是不可行的。即使考虑攻击者可以通过第二原像攻击 [20] 等方式降低实施攻击的难度，攻击的成本对于攻击者来说依然较高。

4.2 中间人攻击

中间人攻击是攻击者通过伪造信息使得节点将攻击者提供的公钥信息误认为是信息接收节点的公钥信息。在不篡改区块链的情况下，这种攻击类似于区块链中的日蚀攻击。攻击者需要控制较多的节点来隔绝受害节点和整个区块链网络之间的联系，建立一个临时的子网络。在 HEILMAN[15] 等人的研究中指出当区块链并不是均匀分布时，攻击者可以利用这一特点，通过控制一定数量的节点从系统中独立出一个子网。在这子网中，多数为恶意节点，恶意节点能够操纵子网中的共识建立，欺骗子网中的普通节点。在 APOSTOLAKI[16] 等人的研究中，通过控制一定数量的路由可以减少攻击所需的资源。攻击者利用在分布不均匀的区块链网络中，节点只能和区块链中有限个节点进行通信。攻击者可以通过向节点填充垃圾地址（如 IP 协议中标记为为未来使用保留的网段），挤占受害节点内存中正常节点的位置。当节点的全部链接全部建立在与恶意节点联系后，攻击者能够对受害节点实施欺骗。根据 HEILMAN 的研究，攻击者需要控制 32 个不同的 /24 IP 段（共 8192 个地址）或拥有 4600 个节点的僵尸网络才能对单个节点有较高的概率实现成功的攻击。而在 APOSTOLAKI 的研究中，使用少于 100 个 /24 IP 能够实现对受害者的攻击。和区块链上的虚拟货币系统不同，基于区块链的公钥系统除了密钥存储服务之外还要求节点提供密钥查询的服务。和虚拟货币交易不同，节点之间的公钥请求存在不可预知性，攻击者无法通过诱导在较短时间内获取有效信息。在无法预计节点发起会话的时间和会话目标的情况下，攻击者需要维持对受害节点欺骗的状态。攻击者除了需要构建一次日蚀攻击之外，

在获得需要的信息前还需要维持一个子网络。由于子网络包含的运算能力和原有的区块链不同，当运算能力差距较大时，节点能够侦测到区块生成的速度发生变化，对这类攻击有一定的预警作用。

4.3 篡改公钥信息

如果攻击者想篡改一个已经存储在区块链中的节点公钥，需要利用区块链的分叉机制，创建一个新的主链来替代包含攻击目标的链。这种攻击实现方式类似于 51% 攻击，需要攻击者拥有超过整个系统总量一半的运算力 [17]。由于哈希碰撞难以实现，攻击者伪造区块和原有区块必然包含不同的哈希值，为了使得伪造的区块链能够得到系统的承认，攻击者需要在伪造的区块后延长足够的链长度，使得包含伪造区块的分支（恶意链）长度大于包含正确信息的节点的分支（即主链）。当恶意链长度超过主链时，恶意链成为新的主链，攻击者就能够诱骗正常节点选择在伪造的链上进行工作。

假设系统中所有节点的运算力为 C，攻击者通过入侵节点获得的运算力为 c。则在生成下一个区块时，区块由攻击者生成的概率为 $q=\frac{c}{C}$，即攻击者能以 q 的概率缩小恶意链与主链之间的长度差。记 $p=1-q$，为区块链系统正常节点发现新的块的概率。假设攻击者不断生成新的区块，攻击者能够成功将恶意链成功转换为主链的概率 r 如公式（1）所示：

$$r = \min\left(1 - \sum_{m=0}^{n} C_{m+n-1}^{m}\left(p^{n}q^{m} - p^{m}q^{n}\right), 1\right) \quad (1)$$

其中 n 代表在攻击发起前区块链系统生成的区块数量，即为了确保区块被区块链所记录所等待的区块数量。攻击者篡改的成功率与攻击者控制的运算力之间的关系如图 3 所示。当 $q>0.5$ 时，由于攻击者获得新的区块的速度大于正常节点，攻击者的篡改一定能够成功，因此图 3 中不包含 $q>0.5$ 的部分。

可以看出攻击成功率和攻击者控制的运算力成正相关的关系，和区块在区块链系统中延迟确认的时间成负相关关系。即使当攻击者控制了系统中 25% 的运算量时，选择适当的延时区块延迟确认时间（如延迟 10 个区块确认信息）仍能够将攻击的成功率降低到较低的范围（1%）。当攻击者控制运算能力比例较低时，攻击的成功率会极大下降。

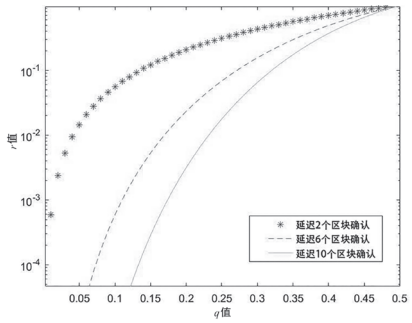

图 3 r 与 q 的关系

5 结束语

本文提出了一个区块链系统的公钥分发系统，利用区块链的抗更改的特性提出一种解决用户公钥的公钥认证问题的方法。本文利用区块链的去中心化的特性，构建去中心化的网络对并发的请求能够有更高的响应效率，当节点数量较多时，节点在开始运行时由于存储的密钥数量较少，响应速度会较慢，经过一定的请求时间后，节点中存储的密钥能够满足用户大部分请求时，节点响应速度会有所提高。分布式网络的形式也让系统能够更好地去适应变化的使用环境。（责编 程斌）

参考文献：

[1] DIFFIE W, HELLMAN M E. New Directions in Cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6):644-654.

[2]SHAMIR A. Identity-based Cryptosystems and Signature Schemes[J].Lecture Notes in Computer Science, 1984, 21(2):47-53.

[3]ALRIYAMI S S, PATERSON K G. Certificateless Public Key Cryptography[EB/OL].https://link.springer.com/chapter/10.1007%2F978-3-540-40061-5_29?LI=true，2017-10-15.

[4]NAKAMOTO S. Bitcoin: A Peer-to-Peer Electronic Cash System [EB/OL]. Available: https://bitcoin.org/bitcoin.pdf，2008-2-15.

[5] LAMPORT L, SHOSTAK R, PEASE M. The Byzantine Generals Problem[J]. ACM Transactions on Programming Languages and Systems, 1982, 4(3): 382 - 401.

[6]DON T,ALEX T.Realizing the Potential of Blockchain [EB/OL]. http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.

pdf,2017-6-10.
[7]JESSE M W. The Future of Financial Infrastructure[EB/OL]. http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf, 2016-8-10.
[8]LARIMER D.Transactions as Proof-of-stake [EB/OL]. http://7fvhfe.com1.z0.glb.clouddn.com/@/wp-content/uploads/2014/01/TransactionsAsProofOfStake10.pdf, 2013-8-10.
[9]LARIMER D.Delegated Proof-of-stake White Paper [EB/OL]. http://www.bts.hk/dpos-baipishu.html, 2014-8-10.
[10] WILLIAM S.Ethereum 'Blockchain Bloat' Could Reach 1TB In 2017 [EB/OL].https://cointelegraph.com/news/ethereum-blockchain-bloat-could-reach-1tb-in-2017, 2017-10-15.
[11] WANG X, FENG D, LAI X, et al. Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD[J]. IACR Cryptology ePrint Archive, 2004 (8): 199-203.
[12] STEVENS M, BURSZTEIN E, KARPMAN P, et al. The First Collision for Full SHA-1[EB/OL]. https://link.springer.com/chapter/10.1007%2F978-3-319-63688-7_19。2017-10-15.
[13] Cryptology Group at Centrum Wiskunde & Informatica (CWI). Google Research Security SHAttered [EB/OL]. https://shattered.io/, 2017-10-15.
[14] WANG Xiaoyun, YIN Yiqun Lisa, YU Hongbo. Finding Collisions in the Full SHA-1 [C] // Victor Shoup. Advances in Cryptology-CRYPTO 2005, August 14-18, 2005, University of California, Santa Barbara. Berlin, Heidelberg: Springer, 2005: 17-36.
[15] HEILMAN E, KENDLER A, ZOHAR A, et al. Eclipse attacks on Bitcoin's peer-to-peer network[C] // USENIX. 24th USENIX Security Symposium, August 12-14, 2015, Washington , USA. Washington : USENIX , 2015:129-144.
[16] APOSTOLAKI M, ZOHAR A, Vanbever L. Hijacking Bitcoin: Routing Attacks on Cryptocurrencies[C]// IEEE.38th IEEE Symposium on Security and Privacy, May 22-25, 2017, San Jose, CA, USA.New York: IEEE, 2017: 375-392
[17] WANG Maoning, DUAN Meijiao. The Second-preimage Attack to Blockchain Based on the Structure of Merkle Hash Tree[J]. Netinfo Security, 2018, 18(1): 38-44.
王卯宁, 段美姣. 基于Merkle哈希树结构的区块链第二原像攻击[J]. 信息网络安全, 2018, 18(1): 38-44.
[18] ROSENFELD M. Analysis of Hashrate-based Double Spending[EB/OL].https://www.researchgate.net/publication/260127064_Analysis_of_Hashrate-Based_Double_Spending, 2014-7-15.
[19]ZHAO Kuo, XING Yongheng. Security Survey of Internet of Things Driven by Block Chain Technology[J]. Netinfo Security, 2017, 17(5): 1-6.
赵阔, 邢永恒. 区块链技术驱动下的物联网安全研究综述[J]. 信息网络安全, 2017, 17(5): 1-6.
[20] MEI Haitao, LIU Jie. Industry Present Situation, Existing Problems and Strategy Suggestion of Blockchain [J]. Telecommunications Science, 2016, 32(11):134-138.
梅海涛, 刘洁. 区块链的产业现状、存在问题和政策建议[J]. 电信科学, 2016, 32(11):134-138.
[21] TANG Chunming, GAO Long. Multi-parties Key Agreement Protocol in Block Chain[J]. Netinfo Security, 2017, 17(12): 17-21.
唐春明, 高隆. 区块链系统下的多方密钥协商协议[J]. 信息网络安全, 2017, 17(12): 17-21.